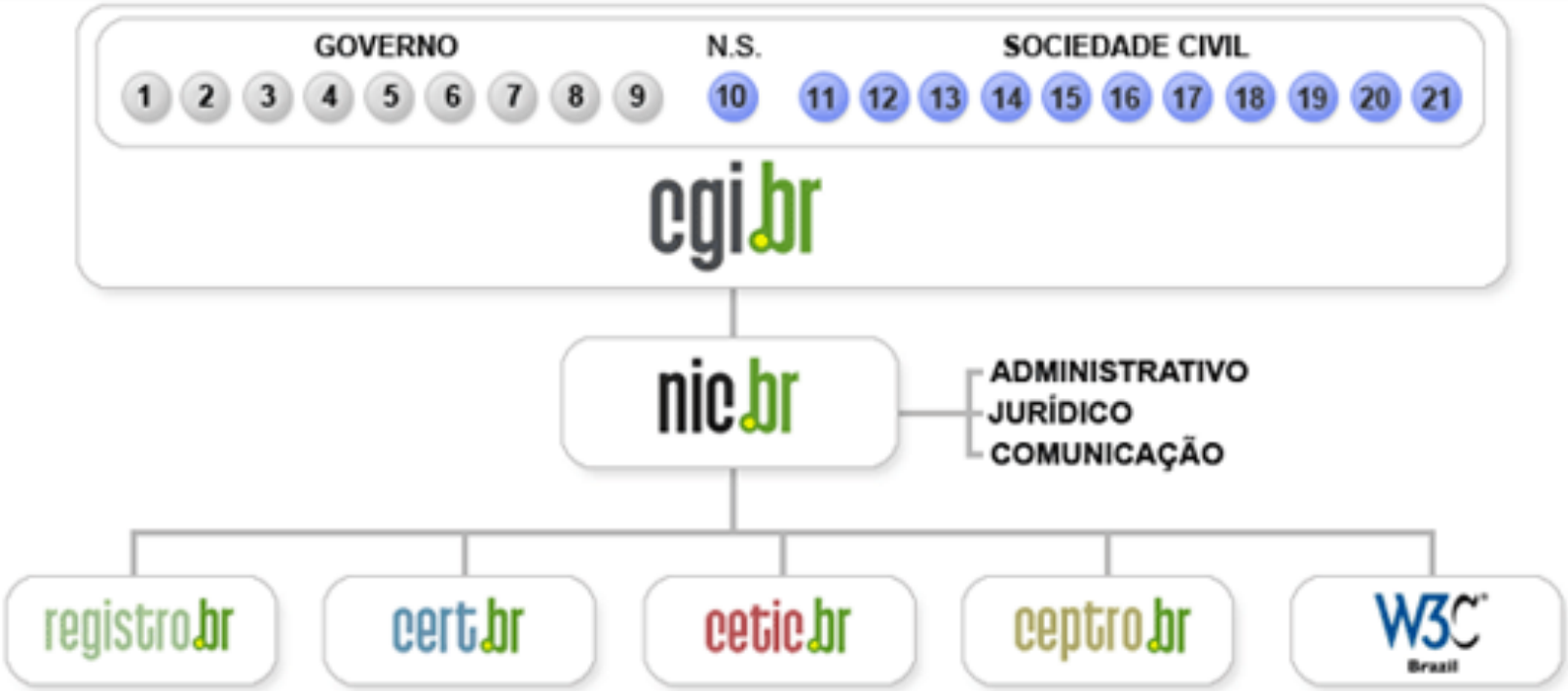
Equilíbrio entre Segurança e Privacidade: Princípios de Segurança

Cristine Hoepers

cristine@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Comitê Gestor da Internet no Brasil – CGI.br

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

http://www.cgi.br/sobre-cg/

CERT.br

Treinamento e Conscientização

- Cursos
- Palestras
- Documentação
- Reuniões

Tratamento de Incidents

- Articulação
- Apoio à recuperação
- Estatísticas

Análise de Tendências

- *Honeypots* Distribuídos
- SpamPots

SEIPartner CERT Courses

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

The Honeynet PROJECT®

Criado em 1997 para:

- Ser um ponto de contato nacional para notificação de incidentes de segurança
- Prover a coordenação e o apoio necessários no processo de resposta a incidentes
- Estabelecer um trabalho colaborativo com outras entidades, como os operadores da justiça, provedores de acesso e serviços e backbones
- Auxiliar novos CSIRTs a estabelecerem suas atividades
- Aumentar a conscientização sobre a necessidade de segurança na Internet

Agenda

- O cenário atual de ataques e ameaças na Internet
- O Modelo de Segurança da Informação
- Desafios

Cenário

Evolução dos Ataques na Última Década

Mudança no enfoque dos atacantes:

- **Ataques a usuários finais**
  - **fraudes, *bots*, *spyware*, etc**
- **Motivação financeira cresce conforme cresce o uso da Internet pela sociedade**

Características das tentativas de fraude com objetivos financeiros:

- **Majoritariamente envolvem *spams***
  - **em nome das mais variadas instituições e com tópicos diversos**
  - **com *links* (URLs) para códigos maliciosos (cavalos de tróia)**
- **Páginas falsas estão voltando a ter números significativos**
- ***Drive-by downloads* sendo usados intensamente no Brasil**
  - **alguns dos casos publicados na mídia:**

    ***sites* principais da Vivo, da Oi e da Ambev**

Fatores que Contribuem para este Cenário

Há grande motivação para ter usuários como alvo e não as empresas:

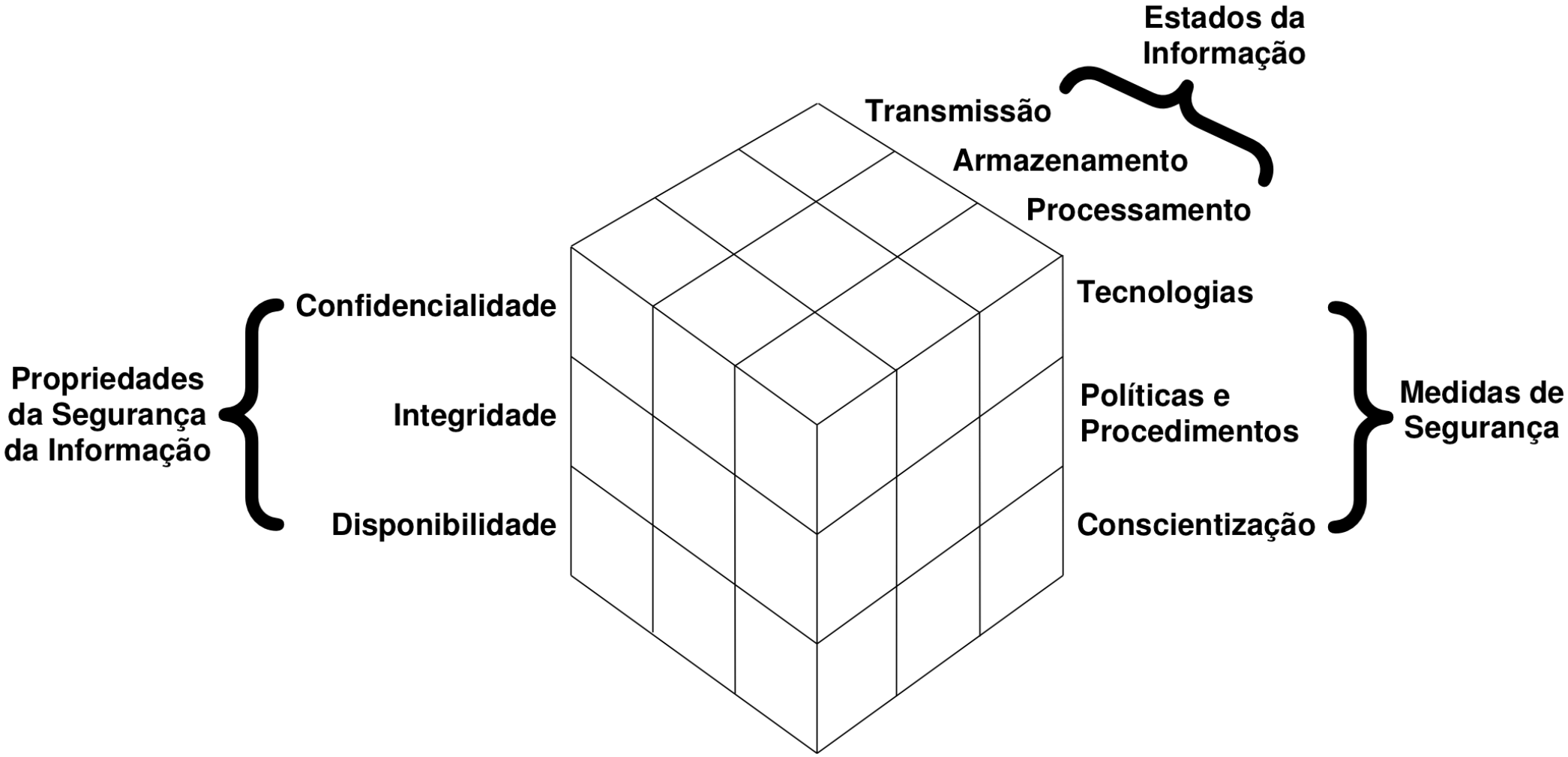
- Tem pouco conhecimento sobre a tecnologia
  - a tecnologia é muito complexa
- É muito difícil entender o que é necessário para se proteger

Fatores de comportamento também contribuem:

- O uso errôneo do termo “virtual” leva muitos a encarar o que ocorre na Internet como fora da vida “real”
- Informações antes restritas ao círculo familiar e/ou de amigos, agora estão *online*
  - twitter, orkut, facebook, etc…

Modelo de Segurança da Informação

Modelo de Segurança da Informação



Especialmente para garantir confidencialidade (e privacidade) é necessario ter controle de acesso, ter logs de quem teve acesso, checar permissões, etc.

Desafios

O que favorece o sucesso dos ataques? (1/2)

Muitas vulnerabilidades de *Software*

- A maioria das quebras de "segurança" nos serviços da "Web 2.0" são por falhas de programação

Uma base muito grande de computadores com *software* desatualizado/vulnerável sendo ativamente abusada por criminosos

- Especialmente em países em desenvolvimento
- Usuários
  - tem dados furtados
  - pagam a conta do uso da Internet por criminosos

O que favorece o sucesso dos ataques? (2/2)

Os serviços *online* e gratuitos tem um preço

- O modelo de negócio é baseado na possibilidade de fazer propaganda
- Para fazer propaganda é necessário ter direitos sobre o conteúdo
  - Quantos já leram a política de privacidade do Google Docs, Dropbox, Facebook, entre outros serviços "da nuvem"?

As pessoas não compreendem o risco de

- Colocar seus dados *online*
- Compartilhar seu dia-a-dia em público
- Não entendem que não é possível ter privacidade e ao mesmo tempo compartilhar as informações em fóruns públicos

De onde vem o debate "*Security vs. Privacy*"?

- **Grande parte das contramedidas são tomadas sem considerar as questões de privacidade**
  - **A maioria sequer funciona ou melhora a segurança, apenas aumenta o controle**
    - **Ex.: "*Unique IDs*", "*RFID passports*", banalização da biometria**
- **Como resultado, medidas válidas e necessárias são questionadas em nome da privacidade**
  - **Mesmo que não afetem a privacidade**
- **Não é necessário comprometer a privacidade para ter mais segurança**
  - **mas registros de eventos (*logs*) são necessários tanto para garantir confidencialidade quanto disponibilidade**
- **Muitas das quebras de privacidade não tem nada a ver com segurança da informação**

O desconhecimento do problema e das soluções gera um embate que não deveria existir.

O Que Fazer?

- **Educação é chave**
  - **Mas não só de usuários**
- **Se não mudarmos**
  - **O modo como desenvolvimento de *software* é ensinado nas Univerdades de computação e engenharia**
  - **E o modo como as empresas desevolvem *software***

Não acho que estaremos melhor em 20 anos

A melhora não virá somente do uso de tecnologias ou da criação de leis, mas sim da compreensão dos problemas e da mudança em como as pessoas usam e desenvolvem a tecnologia.

Informações de Contato

- CGI.br - Comitê Gestor da Internet no Brasil
  http://www.cgi.br/
- NIC.br - Núcleo de Informação e Coordenação do Ponto br
  http://www.nic.br/
- CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
  http://www.cert.br/
- CETIC.br - Centro de Estudos sobre as Tecnologias da Informação e da Comunicação
  http://www.cetic.br/

Cristine Hoepers
cristine@cert.br